DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION
FORT HOOD, TEXAS 76544-5200

AFYB-CG 22 March 2007

MEMORANDUM FOR: SEE DISTRIBUTION

SUBJECT: 4ID, G6 Information Assurance (IA) Policy # 9: Data Integrity / Validation Controls

1. References:

a. AR-25-1, Army Knowledge Management and Information Technology, 15 July 2005.

b. AR 25-2, Information Assurance, 14 November 2003.

c. AR 380-67, Personnel Security Program, 9 September 1988.

d. DoD Directive 8500.1, "Information Assurance (IA)", 24 October 2002.

e. DOD Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003.

f. DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation (C&A) Process, 30 December 1997.

g. DoD CIO Guidance and Policy Memorandum (G& PM) No. 8-8001 - "Global Information Grid (GIG)," 31 March 2000.

h. DoD CIO Guidance and Policy Memorandum No 6-8510, "Department of Defense GIG Information Assurance and Information Assurance Implementation Guide", 16 June 2000.

2. Purpose of Policy:

a. Data integrity and validation is essential to ensuring the accurate transfer of information. The responsibility for maintaining data integrity does not rest with one person, group, or entity, but rather is a shared responsibility. This policy delineates areas of responsibility for maintaining data integrity and validation controls as information is processed and transmitted across the many and various automated information systems (AIS) thresholds within the U.S. Army.

b. 4ID AIS provide an infrastructure supporting the processing, communication, or transfer of a variety of data to and from many sources within and external to 4ID. It is important to ensure that data transmitted across installation transport network (ITN) pathways is secure and can be transported from point-to-point without being altered or compromised in transit. Each Command, Garrison, tenant and individual user of network resources has the responsibility to ensure that the data stored or sent from within their own domain is protected from unauthorized access, modification, disclosure, or destruction while the data is under their care, control, and custody.

c. 4ID designs, implements, operates, and maintains information technology and local and wide area communications infrastructure that supports several commands and thousands of end-users.

d. Advances in high bandwidth, high capacity communications technology have resulted in the interleaving of trusted military communications with openly accessible public, wide area communications networks and Internet communication resources. This policy addresses the use of technology to mitigate a number of those risks.

3. Applicability: This policy applies to all soldiers, civilians, and contractors who plan, deploy, configure, operate, and maintain data communications resources directly or indirectly attached to 4ID networks.

4. Responsibilities:

a. 4ID organizations are responsible for implementing and operating automated information resources as required to support Garrison and Tenant organization data integrity requirements.

b. 4ID will:

(1) Ensure that appropriate data integrity policies are established.

(2) Empower the IAPM to develop a program of audits, system scans, and risk assessments to ensure network and data integrity.

c. The 4ID Information Assurance Manager (IAM) shall verify oversight and compliance with this policy by developing an internal audit, system scan and risk assessment program to ensure all operational components maintain a high level of diligence in protecting the network and ensuring the integrity of the information and infrastructure.

5. Data Integrity and Validation Controls Policy: Consistent data integrity solutions shall be implemented throughout the network. Data integrity solutions encompass, but are not limited to, the following procedures:

a. Strong and consistent user ID and password policies and procedures, as prescribed in the 4ID Password Policy, shall be implemented on all AIS

b. Firewall strategies shall be implemented that 1) deny all port access except those required for specified uses, 2) utilize stateful packet filtering techniques, 3) produce immutable and auditable security and administrative logs that are analyzed and reviewed for abnormal activity, and 4) that application level gateway proxies as required. See Department of Army and 4ID Firewall Policy for further information.

c. Critical network servers shall be configured to maintain a DoD C2 level of security and to produce system and security logs that are analyzed and reviewed for abnormal activity.

d. Dial-up access shall be strictly controlled through the use of acceptable authentication technology ensuring that the DoD C2 level of security is maintained. The data communication channels for remote dial-up access shall be established through a VPN solution to protect user ID's, passwords, and session content from being compromised.

e. All critical systems shall be identified and backed up on a regular basis in accordance with prudent information management practices. Incremental backups shall be made on a nightly basis, with full backups on a weekly basis. At least two sets of system backups shall be created to facilitate storage of one set at a remote off-site location, while one set is retained on site. The first full backup created at the beginning of the month shall be considered the monthly full backup for the previous month and subsequently retained for one year. A test of the ability to restore system backups shall be conducted at least once a month using the most recent archived monthly backup.

f. Critical information shall be stored on network servers and backed up according to the accepted backup strategy. Directory and file level access controls shall be used to prevent unauthorized access to data backed up to the server.

g. Immutable system logs shall be stored on a separate server for review and analysis by system administrators and information assurance personnel.

h. Information assurance and rules of behavior policies shall be developed and shared with the user community in a security awareness program. See 4ID Rules of Behavior Policy for further information.

i. The use of root access shall be restricted to system consoles. Root equivalence may be used if it retains the individual accountability required in a DoD C2 security strategy.

j. Intrusion detection systems (IDS) shall be installed at points where the network is exposed to the general public. IDS technology shall be configured to detect unauthorized access, denial of service attacks, port scanning or other network penetration activity. See 4ID IDS Policy for further information.

k. Individual user communities shall be responsible for implementing policies and procedures to minimize human data entry or data processing errors. Internal checks and balances shall be developed within the user communities to protect data from misuse by authorized users.

l. Strict software and hardware test and evaluation procedures shall be developed and enforced at all levels to ensure equipment or software is not placed into the production environment until it is adequately configured, tested, and evaluated.

m. Strict configuration management procedures shall be adopted to ensure that no unauthorized changes are made to the network systems, software and/or hardware configuration without proper testing, evaluation and approval. Refer to 4ID Operational Controls Policy for further information

n. The need for emergency response capabilities shall be evaluated at all levels of automated information systems operation. Where appropriate, Computer Incident Response Teams shall be trained and available on a 24-hour basis. Procedures for responding to emergencies shall be clearly outlined with action and approval authority established to minimize data loss, damage and operational down time.

o. Administrators shall stay abreast of system patches, O/S upgrades and releases, and review them for keeping systems optimally configured to minimize risk and enhance functionality.

p. A centrally managed virus protection strategy shall be developed that keeps current with virus updates and ensures that all users have the most current version of virus protection. An internal virus protection, response and notification strategy shall be developed in concert with the 4ID IAPM. Virus protection shall be considered one of the highest priorities in maintaining data integrity.

6. Non-compliance: Each Command, Garrison, tenant and end-user is responsible for doing their part to ensure that stored or processed data and the automated information infrastructure are maintained at an optimal level of functionality and operability. Operational complacency can not be tolerated. In the event of an incident involving the compromise of data integrity or confidentiality, the circumstances causing the incident will be evaluated to the extent possible to determine the cause of the breakdown. If it is determined that the breakdown was the result of non-compliance with the above procedures, individuals responsible will be held accountable and appropriate corrective action taken.

7. POC for this policy is the 4ID Information Assurance at DSN 737-0785 or commercial 254-287-0785.

JEFFERY W. HAMMOND
MG, USA
Commanding

DISTRIBUTION:
4ID
Organizations Attached to 4ID Networks